REPORT ON:

Information Technology Disaster Recovery Planning

IAAS | INTERNAL AUDIT & ADVISORY SERVICES

BRITISH COLUMBIA | Ministry of Finance

Table of Contents

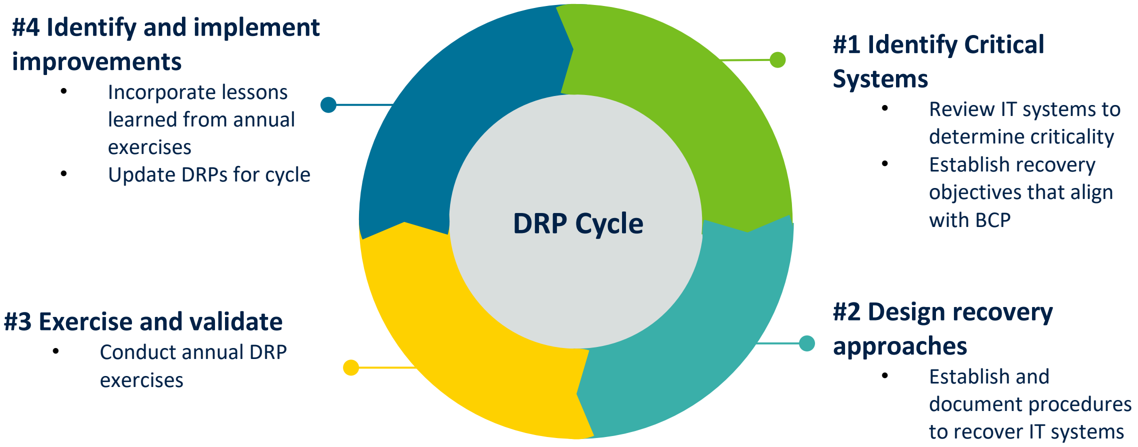
Section **Page No.**

Executive Summary and Overall Conclusion

Information Technology (IT) is vital to many of the public services provided by the Government of British Columbia (Government). The COVID-19 pandemic has put the resilience and continued availability of Government IT systems in the spotlight, as British Columbians have increasingly turned to digital service delivery. A disruption to IT systems may significantly impact the public services people rely on.

IT Disaster Recovery Plans (DRPs) mitigate the risk of such a disruption. A DRP is a written plan for recovering IT systems in response to a major hardware or software failure, data corruption or destruction of facilities. Such plans support the restoration of IT infrastructures and systems that are necessary to the resumption of key government functions. The following figure illustrates the general cycle of a disaster recovery process.

Figure 1: DRP Cycle


#4 Identify and implement improvements
• Incorporate lessons learned from annual exercises
• Update DRPs for cycle
DRP Cycle
#1 Identify Critical Systems
• Review IT systems to determine criticality
• Establish recovery objectives that align with BCP
#3 Exercise and validate
• Conduct annual DRP exercises
#2 Design recovery approaches
• Establish and document procedures to recover IT systems

Source*:* Internal Audit & Advisory Services, based off industry good practices and the CPPM

Two central Government agencies support government services and system resiliency:

- The Office of the Chief Information Officer (OCIO) leads IT strategy, policy and standards for the Government; and

- Emergency Management BC (EMBC) supports the Provincial Business Continuity Management Program, a framework for the development and administration of ministry business continuity processes, including disaster recovery planning.

Under Government policy, ministries are required to develop, maintain and exercise their DRPs.

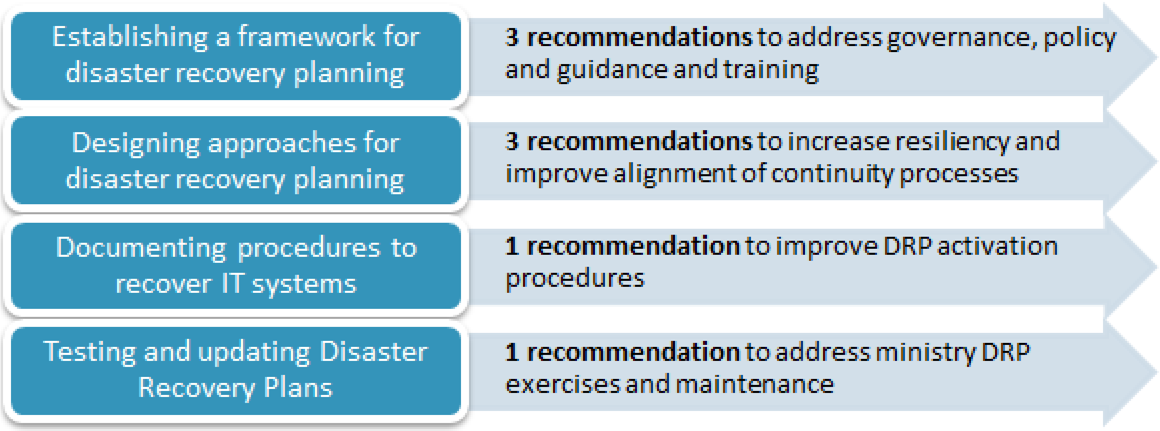
Internal Audit & Advisory Services (IAAS) conducted this review to assess the adequacy of disaster recovery planning in place to recover ministry critical IT systems (Critical Systems) following a significant disruption. For this review, we selected the Ministries of:

- Social Development and Poverty Reduction;
- Children and Family Development;
- Attorney General; and
- Public Safety and Solicitor General.

We found that while these ministries have generally designed their Critical Systems to be resilient, their preparedness to recover from an IT disruption varied. Some Critical Systems have established DRPs that include recovery approaches to meet defined objectives, documented recovery procedures, and regular exercising to validate plans. Other Critical Systems rely on their backups to be recovered after an IT disruption, and do not have documented plans or procedures for recovery. As a result, there is a risk that the recovery of some ministry Critical Systems, which support key government services, could be delayed during a disruption.

This report identifies recommendations that ministries should consider in the development and maintenance of their DRPs. While this review focused on ministry disaster recovery planning, we have advised the OCIO and EMBC of our findings and identified areas where they can further strengthen the support of ministry disaster recovery planning:

Figure 2: IAAS Recommendation Summary



Establishing a framework for disaster recovery planning — **3 recommendations** to address governance, policy and guidance and training

Designing approaches for disaster recovery planning — **3 recommendations** to increase resiliency and improve alignment of continuity processes

Documenting procedures to recover IT systems — **1 recommendation** to improve DRP activation procedures

Testing and updating Disaster Recovery Plans — **1 recommendation** to address ministry DRP exercises and maintenance

Source: IAAS

This review aligns with some of our past reports that have highlighted the importance for Government being prepared against disruptions to services. These include the Review of Critical Systems Standard and the Report on the Provincial Business Continuity Management Program Phase I.

* * *

We would like to thank all ministry staff who participated in and contributed to this review, for their cooperation and assistance.

Stephen Ward, CPA, CA, CIA
Executive Director
Internal Audit & Advisory Services
Ministry of Finance

Introduction

A disruption to the Government of British Columbia's (Government) Information Technology (IT) systems can significantly impact the public services that British Columbians rely on. Disruptions to IT systems can be caused by natural disasters, such as an earthquake or flood, threats to IT systems through malware or ransomware, or other damage to systems or hardware. The COVID-19 pandemic has put the continuity of Government IT systems in the spotlight, as British Columbians have increasingly turned to digital service delivery.

Mission Critical Services are important Government services, that should they not be performed, could lead to loss of life, injury, cause personal hardship to citizens, major damage to the environment, or significant loss of revenue or assets.

Critical Systems are any IT service, system or infrastructure that is necessary to deliver a **Mission Critical Service.**

The Government seeks to safeguard **Mission Critical Services**[1] by planning for their resumption following a disruption. Mission Critical Services could have a significant impact on the Province and it's citizens and may require the support of Mission Critical IT systems (**Critical Systems**).

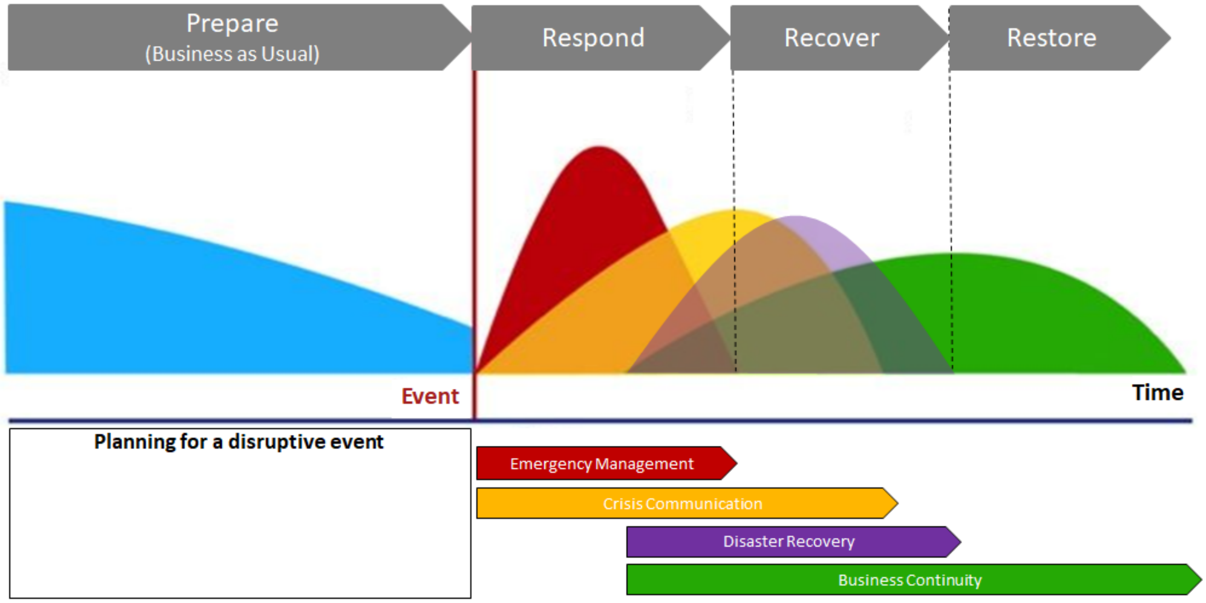
An IT Disaster Recovery Plan (DRP) is a written plan for recovering and restoring Critical Systems following a disruption. Disaster recovery planning as a result, supports the delivery of Mission Critical Services. DRPs include steps to regaining access to IT system, data, and communications after a disruption, and to increase an organization's IT system resiliency. DRPs are generally maintained by ministry technology staff, in collaboration with program areas.

As a result, disaster recovery planning supports the continuous delivery of Mission Critical Services by mitigating the risk of disruptions to these services. Disaster recovery planning is also an integral component of an overall crisis management program.

[1] Mission Critical Services are a sub-set of Critical Services. Critical Services can also include a Business Priority Service, which are those business functions or processes that should they not be performed, could lead to the loss of a major Government service.

The following graph illustrates how the four phases of crisis management complement each other.

Figure 3: Components and Phases of Crisis Management



Source*:* IAAS, adapted from PricewaterhouseCoopers LLP Canada

Emergency management focuses on the prevention and mitigation of, and preparedness for, immediate response to and recovery from a disruptive event, for example, planning the safe evacuation of an office during a fire.

Crisis communication focuses on how an organization's response will be communicated with stakeholders, for example, hosting media conferences to share information on the organization's actions after an earthquake with the public.

Business continuity focuses on the resumption of Mission Critical Services until a return to normal operations is possible by outlining the actions an organization takes to continue or resume these services after a disruption. For example, implementing an alternative work site if an office remains unavailable after a flood.

Purpose, Scope and Approach

The purpose of this review was to assess the adequacy of the disaster recovery processes in place to recover ministry Critical Systems following a disruption. The review evaluated and made recommendations on ministry disaster recovery processes, with a focus on whether ministry DRPs are:

- adequate to recover Critical Systems and services in the event of a disruption;
- communicated to relevant stakeholders; and
- appropriately reviewed and tested to ensure their effectiveness in the event of a disaster.

For this review, we selected the Ministries of:

- Social Development and Poverty Reduction;
- Children and Family Development;
- Attorney General; and
- Public Safety and Solicitor General.

We selected a sample of ministry IT systems that support Mission Critical Services.

This review did not include the disaster recovery planning for the Government's shared IT infrastructure (e.g. data centre facilities, network, enterprise architecture and security services) and enterprise systems (e.g. email and SharePoint) that are centrally managed by the Office of the Chief Information Officer (OCIO).

While this review focused on ministry disaster recovery planning, we have identified areas where OCIO and Emergency Management BC (EMBC) could further support ministry disaster recovery planning. We have shared our findings with staff from OCIO and EMBC.

The review was conducted by Internal Audit & Advisory Services (IAAS), Ministry of Finance. Fieldwork was completed in December 2020.[2] We provided the ministries selected for this review with specific recommendations to help them align their disaster recovery planning with Government policy and industry good practices.[3]

This report consolidates findings from the selected ministries and identifies recommendations they should consider in the development and maintenance of their DRPs.

[2] While IAAS' review was conducted during the COVID-19 pandemic response, the review did not include Government's IT disaster recovery response related to COVID-19.

[3] Industry good practices include: COBIT 2019 framework by the Information Systems Audit and Control Association and the Special Publication 800-34 Rev. 1 by the National Institute of Standards and Technology.

1.0 Establishing a framework for Disaster Recovery Planning

As outlined in Chapter 16 of the Government's Core Policy and Procedures Manual (CPPM), ministries are required to implement a Business Continuity Management Program (BCMP), which includes disaster recovery and business continuity planning. They must provide resources to support DRP development, testing and maintenance, and staff training.

EMBC is responsible for managing the Provincial BCMP, a framework for the development and administration of ministry BCMPs. The OCIO manages the shared IT infrastructure, establishes IT standards, policy and procedures. The OCIO has published the Critical Systems Standard (CSS) that requires ministries to select which of their IT systems are critical. Under the CSS, ministry Critical Systems must have DRPs in place, which are tested annually. As per the CPPM and industry good practices a framework for ministry disaster recovery planning should include a governance structure, policy or guidance, and training.

1.1 Governance and Oversight

Appropriate governance and oversight are important components of disaster recovery planning. Ministry executives evaluate and establish the strategic recovery options, direct senior management in the implementation of these options and monitor achievements. Industry good practices recommend clearly defining roles and responsibilities for effective disaster recovery planning.

The governance structure in place for disaster recovery planning varied amongst the selected ministries. For some, the governance structure was documented in agreements established with IT service providers and included a joint committee comprised of ministry and service provider staff to approve annual DRP exercises. In other selected ministries, it was not evident whether defined structures and processes were established to comply with the CPPM and the CSS requirements related to disaster recovery planning. Without clear responsibilities and processes to deliver DRPs, there is a risk that ministries do not have adequate DRPs or disaster recovery strategies in place to recover their Critical Systems in the event of a disruption. Ministries should define roles and responsibilities as well as processes that can support disaster recovery planning.

EMBC and the OCIO provide support for the Provincial BCMP and IT infrastructure, respectively. High-level requirements through the CPPM and the CSS also offer some direction to ministries. We found that there is no central Government body that currently provides strategic direction to, and support for, ministry disaster recovery planning. The coordination and consistency of ministry disaster recovery planning could be strengthened through a cross-government executive body, including representatives from EMBC and the OCIO, to provide strategic direction and support to ministries.

Recommendation:

(1) Ministries should ensure that executive governance and oversight is in place to support the delivery of disaster recovery planning.

1.2 Policy and Guidance

Establishing policy and guidance helps ensure that disaster recovery planning is consistently applied and staff responsible for developing and maintaining DRPs will understand the expectations associated with their role.

The CPPM and the CSS require that ministries develop, maintain and test DRPs. While this guidance provides some general requirements for disaster recovery planning, there is no complementary guidance that provides specifics to ministries on how to develop, maintain and test a DRP. Additionally, existing information and guidance produced by the OCIO on IT resiliency and disaster recovery planning are limited and not easily accessible.

In some cases, we found that service agreements for the management and support of Critical Systems defined the responsibilities and some requirements for the development, maintenance, approval and testing of DRPs. Outside of these agreements, there is a lack of policy and guidance within selected ministries.

Without sufficient policy and guidance, ministries may inconsistently develop and maintain their DRPs, which can lead to delays in the recovery of a Critical Systems during a disruption. Disaster recovery planning guidance prepared in collaboration between EMBC, the OCIO and ministries would help Government achieve consistency and compliance.

Recommendation:

(2) Ministries should develop guidance for the design, documentation, and testing of Disaster Recovery Plans. Guidance should reflect requirements from the Core Policy and Procedures Manual and the Critical Systems Standard.

1.3 Training and Awareness

To ensure staff are knowledgeable and aware of their roles and responsibilities for disaster recovery planning, it is important to develop and deliver adequate training. The CPPM requires that ministries provide the resources for training and deliver general awareness of disaster recovery planning for staff.

Disaster recovery planning knowledge primarily resides within ministry IT departments and is applied through DRP exercises. Where ministries have developed DRPs, there is a reliance on the IT service providers for managing disaster recovery planning. Overall, we found that selected ministries have not established training or awareness programs on their disaster recovery planning practices.

It would be beneficial for ministries to provide training and increase awareness of disaster recovery processes for key ministry staff (e.g. business continuity and program area staff) in order to ensure a coordinated response during a disruption. For instance, in the event of a large-scale disaster (e.g. earthquake or flood), there is often a need to coordinate both the recovery of Critical Systems and mobilization of staff through a **Business Continuity Plan (BCP)**. Without adequate knowledge sharing, there is a risk that staff may not fully understand their roles, which can impact the ability of the ministries to resume their Critical Systems and Services after a disruption.

A **Business Continuity Plan (BCP)** focuses on the resumption of Mission Critical Services by outlining the actions an organization takes to continue services following a disruption, until a return to normal business operations is possible.

EMBC currently provides training on BCMP to ministry Business Continuity Advisors. However, EMBC does not include disaster recovery planning in its business continuity training nor does the OCIO provide such training. There is a risk that ministries have inadequate or inconsistent understanding of disaster recovery planning requirements and good practices, and how it can be implemented to align with business continuity. It would be beneficial for ministries to develop disaster recovery planning training for their staff involved in disaster recovery and business continuity planning, along with program area staff. This could be achieved through assistance from EMBC and the OCIO and by leveraging existing business continuity training through existing shared platforms (e.g. ministry SharePoint sites) for easy access by relevant staff.

Recommendation:

(3) Ministries should develop and deliver disaster recovery planning training for relevant staff, including business continuity and program area staff.

2.0 Designing Approaches for Disaster Recovery Planning

The CPPM requires that ministries establish the capability to protect and support the timely resumption of Mission Critical Services. This includes disaster recovery and business continuity planning, which are part of a ministry BCMP. To establish the necessary capability for disaster recovery, ministries should identify their recovery objectives for each Critical System, and design recovery approaches to meet such objectives.

2.1 Establishing Recovery Objectives

Developing an approach to recover a system requires identifying objectives for the resumption of Mission Critical Services. These objectives are generally defined as a **Recovery Point Objective (RPO)** and **Recovery Time Objective (RTO)**. RPOs and RTOs are developed through a Business Impact Analysis (BIA), which is a critical component in protecting an organization's resiliency. According to the CPPM and industry good practices, a BIA is used to identify functions to support Mission Critical Services, including linkages to IT systems, interdependencies and key stakeholders.

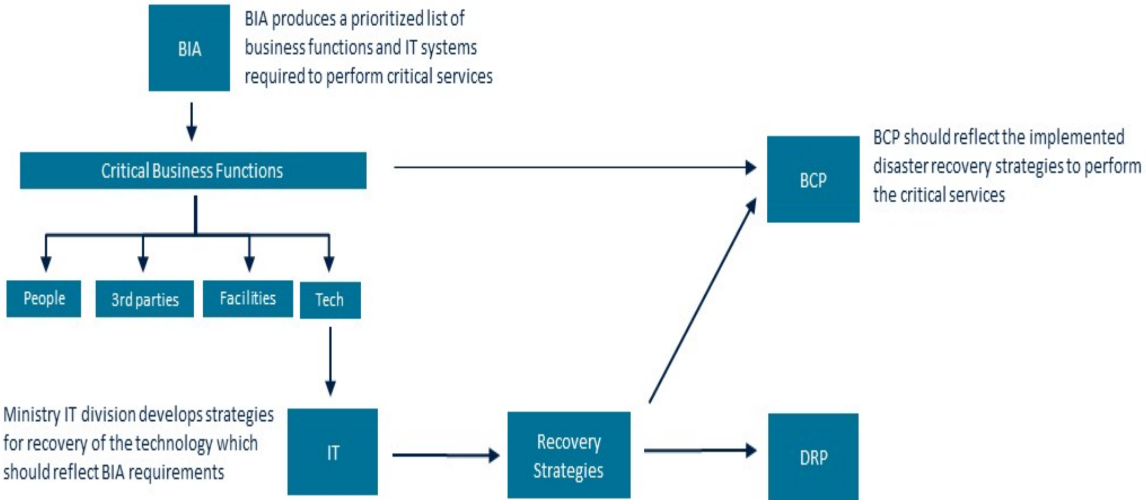
Identifying realistic recovery objectives (e.g. RTO and RPO) for disaster recovery planning helps set expectations for ministries to determine alternative processes for their Mission Critical Services during an IT system disruption. This information is then used to develop recovery strategies for DRPs and BCPs. It is important therefore, that business continuity and disaster recovery strategies and plans align.

Recovery Point Objective is the point in time, prior to a disruption, to which data can be restored from a backup after an outage. The shorter the RPO, the stronger data recovery approach required (e.g. backup frequency, data duplication in separate servers).

Recovery Time Objective is the amount of time that a business function can withstand an interruption before a negative or unacceptable consequence occurs. The shorter the RTO, the stronger the system recovery approach needs to be (e.g. redundant servers, servers in multiple data centers).

The following graphic summarizes how recovery objectives are developed through the BIA, and then incorporated into recovery strategies in the DRP and BCP.

Figure 4: Business Impact Analysis process


BIA
BIA produces a prioritized list of business functions and IT systems required to perform critical services
Critical Business Functions
People
3rd parties
Facilities
Tech
BCP
BCP should reflect the implemented disaster recovery strategies to perform the critical services
Ministry IT division develops strategies for recovery of the technology which should reflect BIA requirements
IT
Recovery Strategies
DRP

Source: IAAS, adapted from PricewaterhouseCoopers LLP Canada

We considered whether business continuity and disaster recovery processes aligned, through a review of business unit BIAs. We found that in some selected ministries, the recovery objectives used to develop DRPs did not always align with those identified by program areas in their BIAs. This contributes to insufficient integration of disaster recovery and business continuity planning in these ministries. For instance, business continuity staff had little input and visibility on their ministries' disaster recovery planning. As a result, there is a risk that during a disaster, BCPs and DRPs diverge, which can hinder ministries' ability to resume their Mission Critical Services. In other ministries, program areas are performing their BIAs to identify the RTOs of their systems; however, RPOs are not identified through this exercise.

Without clear business requirements to develop recovery approaches, there is a risk that program areas' recovery objective expectations may not align with the systems' actual recovery capabilities, leading to unexpected downtime on service delivery and data loss. In addition, enhancing the coordination between business continuity and disaster recovery planning should include the involvement of program area and business continuity staff into disaster recovery planning.

Recommendations:

(4) Ministries should ensure that recovery point and time objectives used for disaster recovery planning are identified by program areas in Business Impact Analyses and are periodically reviewed.

(5) Ministries should include business continuity and program area staff in their Disaster Recovery Plan exercises and planning sessions to strengthen alignment between business continuity and disaster recovery planning.

2.2 Technical Resiliency

Planning for the recovery of a system involves selecting and implementing technologies that deter and reduce the impacts of IT system disruptions, and technologies that enable the recovery of the system within its recovery objectives. Industry good practices suggest that organizations may consider the following according to the criticality and recovery objectives:

- a backup strategy, including a secure offsite location for ready access to backups during a disruption, impacting the primary location;
- the development of an **alternate recovery location** to resume system operations in the event of a catastrophic event that disables the primary location. The alternate location can be set up as a cold, warm or hot site; and
- the use of high availability processes, where duplicate hardware and failover software are built into a system, to eliminate any single point of failure.

Ministries may establish an **alternative recovery location**, available for use in the event of a disaster impacting its primary location by leveraging Government's secondary data centre. Options for alternative recovery locations vary from a fully functioning site, with near real time data replication (i.e. a hot site); a site with established IT infrastructure, such as servers or storage, and ready to be activated during a disruption (i.e. a warm site), or; a site with basic communication and power infrastructure to support the recovery (i.e. a cold site).

When selecting a recovery approach and associated technologies, organizations should consider the criticality of their systems, recovery objectives, likelihood of threats, and cost of the technologies. The OCIO offers technical services for ministries to incorporate into their recovery approaches, such as technical support beyond business hours, and services that enable ministries to recover their servers in an alternate data centre.

Ministries have generally designed their Critical Systems with the goal of being technically resilient by leveraging the OCIO's services, including high-availability technology and backups. We also found that the recovery approach for some Critical Systems relies on system file and data backup. In the event of data corruption or system failure, ministries can expect to limit their data loss and support the recovery of their Critical Systems; however, it is uncertain whether they will be able to meet their recovery objectives in various disaster scenarios. Considering recovery approaches for relevant disaster scenarios will help improve the recoverability of Critical Systems.

We also identified that selected ministries have not always considered applicable technical services offered by the OCIO to strengthen their recovery approaches, and their approaches are not always consistent between Critical Systems. The OCIO's technical services can include a backup strategy, the use of an alternate data centre or the use of redundant servers. Ministries should document their rationale to demonstrate that their approaches are sufficient and meet program areas' needs.

Recommendation:

(6) Ministries should develop and regularly review their recovery approaches for Critical Systems to ensure consistency with recovery objectives.

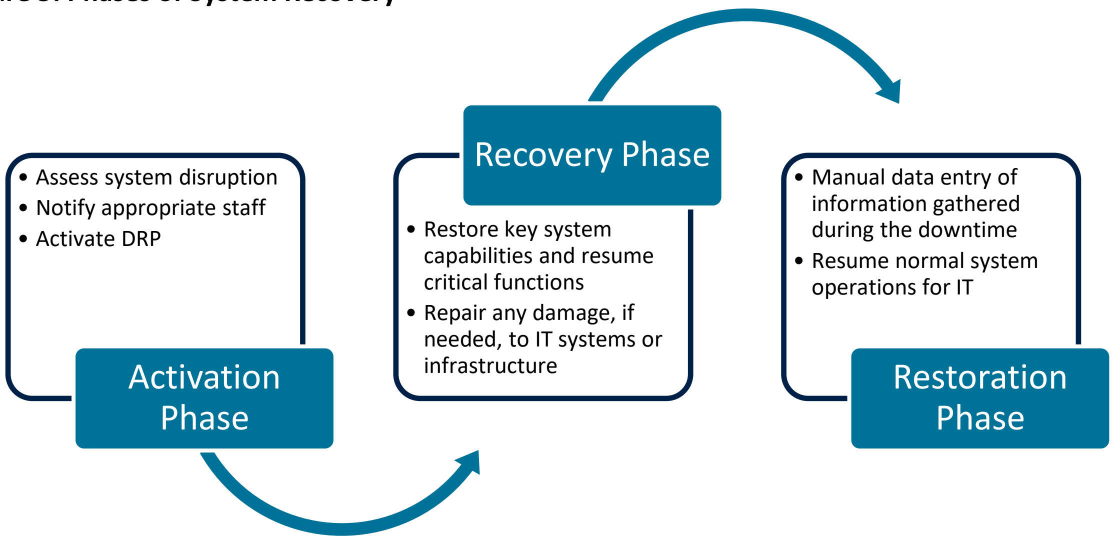
3.0 Documenting Procedures to Recover IT Systems

The CPPM requires that ministry DRPs document how they will resume their Mission Critical Services following a disruption. Developing DRPs is a critical step in the process of implementing comprehensive disaster recovery planning.

A DRP details roles, responsibilities, teams, communications and procedures associated with restoring an IT system following a disruption. This mitigates the risk of errors and reliance on a limited pool of knowledgeable staff, who may be unavailable to recover the system. In addition, this helps ensure a coordinated and effective recovery and enables the evaluation of the recovery process through regular testing and continuous improvement.

The cause of disruptions to IT systems can vary, from natural disasters, IT threats through malware or ransomware, or damage to software or hardware. The results of such disruptions can significantly impact business processes, leading to delays in the Critical Service delivery. Industry good practices recommend that DRPs develop and document the procedures to recover systems following key disaster scenarios. The following graph describes the three phases of a system recovery:

Figure 5: Phases of System Recovery



Activation Phase
- Assess system disruption
- Notify appropriate staff
- Activate DRP

Recovery Phase
- Restore key system capabilities and resume critical functions
- Repair any damage, if needed, to IT systems or infrastructure

Restoration Phase
- Manual data entry of information gathered during the downtime
- Resume normal system operations for IT

Source*:* IAAS, adapted from the Special Publication 800-34 Rev. 1 by the National Institute of Standards and Technology

We reviewed documentation of selected ministry recovery procedures. We found that some Critical Systems were supported by procedures documented in their DRPs based on key scenarios. Such DRPs were available on the selected ministries' and their service providers' networks so that they could be accessible to relevant staff during a disruption. We also found that other systems did not have documented procedures. This presents a risk that some ministry systems may not be recovered within their recovery objectives.

The DRP of a Critical System should clearly identify the roles, responsibilities and staff assigned to the recovery of that system. This includes identifying the authority responsible for activating the DRP, and alternate staff, should primary staff be unavailable. We found that the responsibility for activating selected ministry DRPs was not always clearly identified. In times of emergency, this may lead to delays in DRP activation, impacting the timeliness of recovery efforts.

For Critical Systems with developed DRPs, there were clearly documented recovery procedures. In these cases, selected ministry IT and service provider staff had good knowledge of their roles and responsibilities, as well as the recovery and restoration procedures. For Critical Systems without a DRP, we identified that existing processes within selected ministries could be leveraged to support the development of DRPs. This includes processes related to the management of major incidents, incident notification, knowledge sharing between IT team members and systems support documentation. Without adequate documentation of recovery procedures and identification of staff roles and responsibilities, there is a risk that recovery efforts lose their effectiveness in times of emergency.

Recommendation:

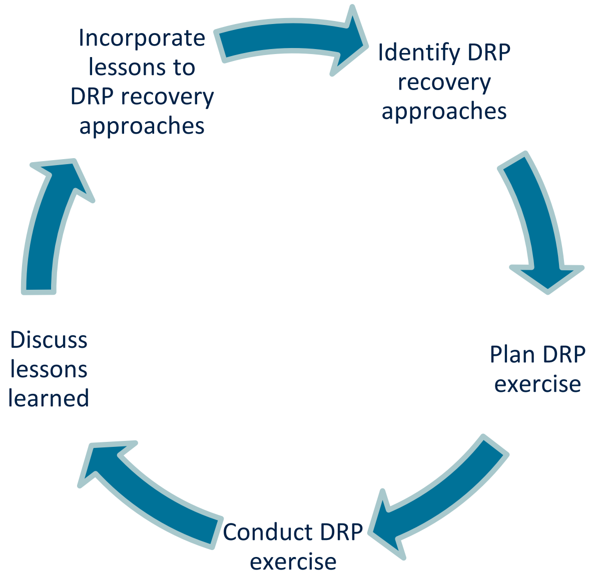
(7) Ministry Disaster Recovery Plans should document their activation, recovery and restoration procedures, as well as associated roles and responsibilities with current contact information, for each Critical System.

4.0 Testing and Updating Disaster Recovery Plans

DRP exercises confirm the viability of recovery procedures, by testing plans identified in ministry DRPs. DRP exercises may vary from conducting full recovery tests of an IT system to smaller scale exercises, such as exercises validating communication strategies for key DRP personnel. The CPPM requires that ministry DRPs are exercised and reviewed and updated on an annual basis.

We found that systems with existing DRPs are exercised annually. Exercises test the full system recovery and include conducting failover exercises that recover systems in their recovery environment (e.g. alternate datacentre, alternate servers). Smaller scale exercises that, for instance, test the viability of communication strategies could increase ministries' confidence in their ability to activate their DRPs and recover their Critical Systems at any date and time.

Figure 6: DRP exercise cycle


Identify DRP recovery approaches
Plan DRP exercise
Conduct DRP exercise
Discuss lessons learned
Incorporate lessons to DRP recovery approaches

Source: IAAS, based off industry good practices and the CPPM

DRP exercises require extensive planning including collaboration between key technical staff, service providers, the OCIO, and other organizations (i.e. other ministries, crown corporations, central agencies) that may have dependencies with the systems. These exercises provided a valuable learning experience for staff involved. Involving business continuity and program area staff in these exercises would increase the awareness of DRP practices beyond the IT department and provide opportunity for these staff to raise potential concerns.

As exercises help identify gaps and validate assumptions in disaster recovery approaches and procedures, lessons learned activities identify the actions to resolve these gaps and eventually strengthen the recovery. For example, a ministry may identify that controls are missing in the DRPs to verify the integrity of recovered data or that staff contacts and notification procedures documented in the DRPs are outdated or inadequate.

We observed that the documentation of the results of DRP exercises, including the lessons learned, contained limited information on the particular finding. Providing more information on DRP exercise results would allow ministry senior management and executives to better understand the identified gaps and collaborate on actions required to continuously improve DRPs.

For Critical Systems without developed DRPs, we found that selected ministries have tested the effectiveness of their high-availability design and tested the restoration of their data backups. Selected ministries did not report any significant issues on these tests. However, there was no schedule to perform these tests regularly and only limited documentation of the test results.

The CPPM requires that ministries review their recovery capabilities and update their DRPs annually, or more often, as changes warrant. Without regular maintenance, recovery capabilities may become misaligned with program areas' needs, and procedures documented in DRPs can lose their effectiveness. For Critical Systems with developed DRPs, we found that plans are updated on at least an annual basis, often preceding and following a DRP exercise. This practice is in alignment with the CPPM and industry good practices.

Without regular testing of the systems’ capabilities to sustain and recover from a system outage or major IT disruption, ministries do not have the sufficient assurance that their recovery approaches and procedures are adequate. Once ministries have developed DRPs for their Critical Systems, they should exercise them periodically, conduct lessons-learned and update them accordingly. In the absence of documented DRPs, ministries should regularly test and document the effectiveness of their Critical Systems’ high-availability design and data restoration from backup. Regular exercises confirm the viability and adequacy of recovery approaches identified in ministry DRPs in the event of a disruption.

Recommendation:

(8) Ministries should exercise their Disaster Recovery Plans on an annual basis or as changes warrant. Lessons learned from Disaster Recovery exercises should then be incorporated into regular updates to the Disaster Recovery Plans.

Appendix A- Summary of Recommendations

1	Ministries should ensure that executive governance and oversight is in place to support the delivery of disaster recovery planning.
2	Ministries should develop guidance for the design, documentation, and testing of Disaster Recovery Plans. Guidance should reflect requirements from the Core Policy and Procedures Manual and the Critical Systems Standard.
3	Ministries should develop and deliver disaster recovery planning training for relevant staff, including business continuity and program area staff.
4	Ministries should ensure that recovery point and time objectives used for disaster recovery planning are identified by program areas in Business Impact Analyses and are periodically reviewed.
5	Ministries should include business continuity and program area staff in their Disaster Recovery Plan exercises and planning sessions to strengthen alignment between business continuity and disaster recovery planning.
6	Ministries should develop and regularly review their recovery approaches for Critical Systems to ensure consistency with recovery objectives.
7	Ministry Disaster Recovery Plans should document their activation, recovery and restoration procedures, as well as associated roles and responsibilities with current contact information, for each Critical System.
8	Ministries should exercise their Disaster Recovery Plans on an annual basis or as changes warrant. Lessons learned from Disaster Recovery exercises should then be incorporated into regular updates to the Disaster Recovery Plans.

Appendix B - Abbreviations

BCP	Business Continuity Plan
BCMP	Business Continuity Management Program
BIA	Business Impact Analysis
CSS	Critical Systems Standard
CPPM	Core Policy and Procedures Manual
Critical Systems	Ministry Critical IT systems
DRP	Disaster Recovery Plan
EMBC	Emergency Management BC
Government	Government of British Columbia
IAAS	Internal Audit & Advisory Services
IT	Information Technology
OCIO	Office of the Chief Information Officer
RPO	Recovery Point Objective
RTO	Recovery Time Objective